UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/529,989	10/20/2005	Mickael Allain	5284-55PUS	2271

27799 7590 04/03/2009

COHEN, PONTANI, LIEBERMAN & PAVANE LLP
551 FIFTH AVENUE
SUITE 1210
NEW YORK, NY 10176

EXAMINER
CHAI, LONGBIT

ART UNIT	PAPER NUMBER
2431	

MAIL DATE	DELIVERY MODE
04/03/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Advisory

1. The claim amendments filed on 3/25/2009 in response to the Final action submitted on 1/28/2009, to restore the original scope of claim limitations, filed on 3/31/2005, have been entered and thereby, the first paragraph of 35 U.S.C. 112 rejection has been withdrawn.
2. As per claim 1, Applicant asserts (a) Haukka fails to teach a remote call manager server decrypting a control code, comparing a parameter extracted from the decrypted control code, and setting up a call as a function of the comparison (Remarks: Page 6 Item # 2) and (b) Haukka fails to teach a database that includes an address identifying the telecommunications terminal (Remarks: Page 6 Item # 4). Examiner respectfully disagrees with the following rationale:

- Regarding argument–(a), Haukka teaches (i) both the user equipment (UE) and the visiting network (CSCF) calculates a temporary identity index using a hash function H(x) based upon the public identity x of the sender (UE) (Haukka: Para [0017] Line 23 – 26), (ii) the temporary identity index is created and placed into a SIP message which is then encrypted, before the transmission, using an encryption algorithm determined during the registration of the UE (Haukka: Para [0009] Line 1 – 9), and (iii) during a registration period, a set of security suite (including the encryption algorithm, encryption key and temporary identity index) is saved in both of the user equipment (UE) and the visiting network (CSCF) (Haukka: Para [0017] Line 29 – 35 and Para [0009] Line 1 – 9). Therefore, Examiner notes a control code (i.e. a hash value of a public identity of a sender UE as a temporary identity index) is indeed created and encrypted that matches the claim language as recited in the claim 1. Furthermore, Applicant argues “Haukka

does not teach a method of “verifying the identity of the sender", but rather teaches a method of protecting the confidentiality of the sender” (Remarks: Page 9 / 1st Para). Examiner respectfully disagrees because the purpose of the registration between a UE and a visiting network (CSCF) is to authenticate a sender (UE) is indeed *a registered user* (UE) before the authorization of data exchange can be started and as such Applicant's arguments are respectfully traversed.

- Regarding argument–(b), Haukka teaches (i) during a registration period, a set of security suite (including the encryption algorithm, encryption key and temporary identity index (i.e. a public identity of the sender (UE)) is saved in a memory of the user equipment (UE) and a memory of the visiting network (CSCF) (Haukka: Para [0017] Line 29 – 35 / Line 25 – 26) and Examiner notes a database is merely a memory storage area with a collection of an organized body of information data and as such Haukka does teach a database that includes an address identifying the telecommunications terminal.